UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,061	04/28/2005	Apostolis Salkintzis	CE10337EP	4449

22917 7590 02/21/2008

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
02/21/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com
APT099@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	10/533,061	SALKINTZIS, APOSTOLIS	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/05/2006, 04/28/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-25 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, I 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 01/05/2006 and 04/28/2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Preliminary Amendment

3. The preliminary amendment submitted on 04/28/2005 is duly noted.

Priority

4. The claim for priority from EPO 02386016.6 filed on 11/29/2002 is duly noted.

Claim Objections

5. Claims 1-25 are objected to because of the following informalities: claims 2-24 state *"A method"* they should state *"The method"*, claim 1, line 8 states *"of GPRS authentication messages"* if it is the same as in line 6 then it should state *"of the GPRS authentication messages"*, claim 2 line 1 and line 2 state *"a GPRS communication"* and *" authorising the*

access port for GPRS communication only" they should state *"the GPRS communication"* and *"authorizing the access point for GPRS communication unit only"*, claims 7, 8, 10-13, 16, 18, and 24 state *"a local network"* they should state *"the local network"*, claim 15 and 18 state *"the access port"* it should state *"the access point"*, claim 16 and 25 state *"encapsulating GPRS authentication"* it should state *"encapsulating the GPRS authentication"*, and claims 15 and 18 state *"authorising the"* it should state *" authorizing the"*. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claim 25 recites the limitation *"the access point"* in lines 3 and 7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-19, 21, 22, and 25 are rejected under 35 U.S.C. 102(a) as being anticipated by US 7107620 (Haverinen).

As to claim 1, Haverinen discloses a method of authenticating a GPRS communication unit on a GPRS communication system through an access point of a local network, the method

comprising the steps of: the GPRS communication unit attaching to the access point using a local network protocol (Haverinen column 9, lines 56-63: The actual type of the telecommunications network is irrelevant. GSM is used as an example, but the network type could as well be Universal Mobile Telecommunications System (UMTS) or GSM with General Packet Radio Service (GPRS). Actually, GPRS can be understood as an extension to GSM rather than an independent network in the sense that GPRS operates using GSM radio access network and GSM authentication methods);

and authenticating the GPRS communication unit by communicating GPRS authentication messages between the GPRS communication unit and a GPRS authentication element through the access point by encapsulation of GPRS authentication messages in local network authentication messages (Haverinen column 3, lines 5-41: According to a first aspect of the invention there is provided an authentication method for authenticating a mobile node to a packet data network, comprising the steps of: providing the mobile node with a mobile node identity and a shared secret specific for the mobile node identity and usable by a telecommunications network; providing the mobile node with a protection code; sending the mobile node identity and the protection code from the mobile node to the packet data network; providing the packet data network with authentication information usable by the telecommunications network, the authentication information comprising a challenge and a session secret corresponding to the mobile node identity and derivable using the challenge and the shared secret; forming cryptographic information using at least the protection code and the session secret; sending the challenge and the cryptographic information from the packet data network to the mobile node; checking at the mobile node the validity of the cryptographic

information using the challenge and the shared secret; generating at the mobile node the session secret and a first response corresponding to the challenge, based on the shared secret; sending the first response to the packet data network; and checking the first response for authenticating the mobile node).

As to claim 2, Haverinen discloses a method of authenticating a GPRS communication unit as claimed in claim 1 further comprising the step of authorising the access port for GPRS communication only if the GPRS communication unit is authenticated by the GPRS authentication element (Haverinen column 22, lines 9-13: If the PAC receives a positive acknowledge message ACK confirming successful authentication, it completes the authentication by opening the access to the Internet. If the PAC receives a negative acknowledge message NACK, it refuses to open access to the Internet).

As to claim 3, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the access point requesting an identity from the GPRS communication unit (Haverinen column 2, lines 40-43: The IP network also includes a special security server (SS), to which a message about a new user is transmitted when a subscriber attaches to the IP network).

As to claim 4, Haverinen discloses a method of authenticating as claimed in claim 2 wherein the step of authenticating comprises the step of the GPRS communication unit transmitting an identity to the access point (Haverinen abstract: In the method, the mobile node sends its subscriber identity to the packet data network together with a replay attack protector).

As to claim 5, Haverinen discloses a method of authenticating as claimed in claim 3 wherein the identity includes a GPRS subscriber identity (Haverinen abstract: In the method, the

mobile node sends its subscriber identity to the packet data network together with a replay attack protector).

As to claim 6, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the access point communicating an access message to the GPRS authentication element indicating that the GPRS communication unit has attached to the access point (Haverinen column 21, lines 5-13: FIG. 9 shows the major signalling steps of the system of FIGS. 7 and 8. The process of authenticating the MT to the PAC is typically triggered when the MT attempts to connect to the public access network. In this case, the MT acquires an IP address via a dynamic host configuration protocol (DHCP) server (not shown). The DHCP protocol and appropriate servers are well known in the art. The authentication has to be completed before the network beyond the PAC can be accessed).

As to claim 7, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the communicating a GPRS Authentication Initiation message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication Initiation message encapsulated in a local network authentication message from the access point to the GPRS communication unit (Haverinen column 21, lines 13-17: The MT triggers the authentication by roaming software. In an alternative embodiment, the authentication is automatically triggered when the MT tries to access to the network using SIM authentication and the roaming application is running).

As to claim 8, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step communicating a GPRS Attach Request message encapsulated in a local network authentication message from the GPRS communication

unit to the access point, and the step of communicating the GPRS Attach Request message from the access point to the GPRS authentication element (Haverinen column 8, lines 63-67 and Figure 10: (Step 401) The MT sends an MT originated authentication starting request MT_PAC_AUTHSTART_REQ containing the NAI having the IMSI. The request typically also contains a protection code MT_RAND (known also as nonce in the context of mobile IP)).

As to claim 9, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the GPRS authentication element retrieving authentication data associated with the GPRS communication unit from a Home Location Register (Haverinen column 23, lines 5-12 and Figure 10: Step 403) The GAGW obtains the GSM triplets from the home GSM telecommunications network. One triplet suffices, but the GSM telecommunications network may return a plurality of triplets, in which case either some of the triplets are discarded or stored for later use, or more advantageously, they all are used to generate a stronger key. The home GSM telecommunications network is recognised using the NAI).

As to claim 10, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the communicating a GPRS Authentication and Ciphering Request message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication and Ciphering Request message encapsulated in a local network authentication message from the access point to the GPRS communication unit (Haverinen column 23, lines 13-34 and Figure 10: (Step 404) The GAGW generates K, using an encryption algorithm, of at least the GSM session key(s) Kc. Advantageously, the MT_RAND is also used in the encryption. The GAGW encrypts the GSM

RAND(s) of the GSM triplets, computes a cryptographic checksum, or a Message Authentication Code MAC, based on the RAND(s) and the K, and prepares an authentication start response message GAGW_PAC_AUTHSTART_RESP. The encryption between the GAGW and the PAC is based on their own shared secret. (Step 411) The GAGW sends to the PAC an authentication start response message GAGW_PAC_AUTHSTART_RESP containing the RANDs, the MAC, the MT_RAND, a billing information code and a billing information MAC computed for the billing information code. Typically, the authentication start response message additionally contains a field for a session timeout parameter for determining the validity period of the new K to be generated and a field for the state of the session. (Step 412) The PAC forwards to the MT the authentication start response message GAGW_PAC_AUTHSTART_RESP as a PAC_MT_AUTHSTART_RESP message).

As to claim 11, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step communicating a GPRS Authentication and Ciphering Response message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Authentication and Ciphering Response message from the access point to the GPRS authentication element (Haverinen column 23, lines 53-63 and Figure 10: (Step 421) The MT generates and sends an MT_PAC_AUTHANSWER_REQ message to the PAC. The message contains in the state field an answer of the user showing whether the user accepted the billing for the service, the MAC of the SRESs, a MAC of the billing code, and the MT_RAND (as all the messages sent during an authenticating session). (Step 422) The PAC generates a PAC_GAGW_AUTHANSWER_REQ containing the data of the

MT_PAC_AUTHANSWER_REQ message and additionally the NAI and the IP address of the PAC).

As to claim 12, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the communicating a GPRS Attach Accept message from the GPRS authentication element to the access point, and the step of communicating the GPRS Attach Accept message encapsulated in a local network authentication message from the access point to the GPRS communication unit (Haverinen column 24, lines 1-24 and Figure 10: (Step 424) If the GAGW gets a positive answer to the test of the previous step, it generates the access key Kpac_MT in a manner similar to that used by the MT in step 416 and then proceeds to the step 431. (Step 431) The GAGW sends to the PAC a message GAGW_PAC_AUTHANSWER_RESP_OK. The message contains the MT_RAND and codes filter_id, Kpac_MT and SIGNresult. The filter_id code is optional and indicates the user class of the subscriber. This can be used in defining a QoS, for example a high quality connection for more paying business users. The SIGNresult is a MAC of the data in the message for ultimately verifying to the MT that the reply from the GAGW is not altered on the way to the MT. (Step 441) The PAC responds to the GAGW by a PAC_GAGW_STARTBILLING_REQ message requesting the GAGW to start the billing. The message contains the NAI and a session ID (the MT_RAND). (Step 442) The GAGW checks the answer from the MT for verifying that the MT has permitted the billing. (Step 451) If the MT has permitted the billing, the GAGW sends to the PAC a message GAGW_PAC-STARTBILLING_RESP_OK to indicate the start of billing. (Step 452) The PAC sends to the MT a PAC_MT_AUTHANSWER_RESP_OK message containing the SIGNresult).

As to claim 13, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of communicating a GPRS Attach Complete message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Complete message from the access point to the GPRS authentication element (Haverinen column 24, lines 31-33 and Figure 10: A method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of communicating a GPRS Attach Complete message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Complete message from the access point to the GPRS authentication element).

As to claim 14, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the GPRS authentication element communicating with a Home Location Register to perform a GPRS location update (Haverinen column 19, lines 60-67: As is known from the GSM, the home GSM network stores customer information, such as authentication codes and user identity. Typically, this information is stored in a GSM Home Location Register (HLR) of an MSC. The GSM telecommunications network operator provides the IP based authentication and charging interface for one or several WISP operators, possibly also or only for corporate access solutions).

As to claim 15, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of communicating an authentication success message from the GPRS authentication element to the access point, and the step of authorising the access port for GPRS communication for the GPRS communication unit in

response to receiving the authentication success message (Haverinen column 24, lines 5-6: The GAGW sends to the PAC a message GAGW_PAC_AUTHANSWER_RESP_OK).

As to claim 16, Haverinen discloses a method of authenticating as claimed in claim 1 wherein communication of GPRS authentication messages from the GPRS authentication element to the access point are by encapsulating GPRS authentication messages in local network authentication messages (Haverinen column 20, lines 54-62: The MT-PAC interface is an IP based interface that is provided with authentication functionality. The authentication is designed so that it can be embedded in a well-known standard IP protocol or implemented as an extension to the existing protocol. The MT and PAC are identified using their IP addresses in this interface. The PAC-GAGW interface is an IP based interface that uses a suitable authentication protocol. Typically, a single GAGW supports several PACs simultaneously).

As to claim 17, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the authentication is part of a routing area update (Haverinen column 27, lines 40-45: In example 2, the functionality for the authenticator entity which is responsible for authenticating a terminal is located in a network layer router. Alternatively, the functionality is in a link layer element, such as a WLAN access point, in which case the interface between the MT and the WLAN access point is based on a link layer protocol rather than IP).

As to claim 18, Haverinen discloses A method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the steps of: communicating a GPRS Authentication Initiation message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication Initiation message encapsulated in a local network authentication message from the access point to the GPRS communication unit;

followed by the step of (Haverinen column 21, lines 6-8: The process of authenticating the MT to the PAC is typically triggered when the MT attempts to connect to the public access network):

communicating a GPRS Attach Request message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Request message from the access point to the GPRS authentication element; followed by the step of (Haverinen column 22, lines 63-67 and column 23, lines 1-4: (Step 401) The MT sends an MT originated authentication starting request MT_PAC_AUTHSTART_REQ containing the NAI having the IMSI. The request typically also contains a protection code MT_RAND (known also as nonce in the context of mobile IP). (Step 402) The PAC receives the MT_PAC_AUTHSTART_REQ from the MT and requests for GSM triplets by sending to the GAGW a message PAC_GAGW_AUTHSTART_REQ, also containing the NAI and the MT_RAND.):

communicating a GPRS Authentication and Ciphering Request message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication and Ciphering Request message encapsulated in a local network authentication message from the access point to the GPRS communication unit; followed by the step of (Haverinen column 23, lines 5-34: Step 403) The GAGW obtains the GSM triplets from the home GSM telecommunications network. One triplet suffices, but the GSM telecommunications network may return a plurality of triplets, in which case either some of the triplets are discarded or stored for later use, or more advantageously, they all are used to generate a stronger key. The home GSM telecommunications network is recognised using the NAI. (Step 404) The GAGW generates K, using an encryption algorithm, of at least the GSM session key(s) Kc.

Advantageously, the MT_RAND is also used in the encryption. The GAGW encrypts the GSM RAND(s) of the GSM triplets, computes a cryptographic checksum, or a Message Authentication Code MAC, based on the RAND(s) and the K, and prepares an authentication start response message GAGW_PAC_AUTHSTART_RESP. The encryption between the GAGW and the PAC is based on their own shared secret. (Step 411) The GAGW sends to the PAC an authentication start response message GAGW_PAC_AUTHSTART_RESP containing the RANDs, the MAC, the MT_RAND, a billing information code and a billing information MAC computed for the billing information code. Typically, the authentication start response message additionally contains a field for a session timeout parameter for determining the validity period of the new K to be generated and a field for the state of the session. (Step 412) The PAC forwards to the MT the authentication start response message GAGW_PAC_AUTHSTART_RESP as a PAC_MT_AUTHSTART_RESP message):

communicating a GPRS Authentication and Ciphering Response message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Authentication and Ciphering Response message from the access point to the GPRS authentication element; followed by the step of (Haverinen column 23, lines 53-63: (Step 421) The MT generates and sends an MT_PAC_AUTHANSWER_REQ message to the PAC. The message contains in the state field an answer of the user showing whether the user accepted the billing for the service, the MAC of the SRESs, a MAC of the billing code, and the MT_RAND (as all the messages sent during an authenticating session). (Step 422) The PAC generates a PAC_GAGW_AUTHANSWER_REQ containing the data of

the MT_PAC_AUTHANSWER_REQ message and additionally the NAI and the IP address of the PAC):

communicating a GPRS Attach Accept message from the GPRS authentication element to the access point, and the step of communicating the GPRS Attach Accept message encapsulated in a local network authentication message from the access point to the GPRS communication unit; followed by the step of (Haverinen column 24, lines 5-13 and 23-24: (Step 431) The GAGW sends to the PAC a message GAGW_PAC_AUTHANSWER_RESP_OK. The message contains the MT_RAND and codes filter_id, Kpac_MT and SIGNresult. The filter_id code is optional and indicates the user class of the subscriber. This can be used in defining a QoS, for example a high quality connection for more paying business users. The SIGNresult is a MAC of the data in the message for ultimately verifying to the MT that the reply from the GAGW is not altered on the way to the MT… (Step 452) The PAC sends to the MT a PAC_MT_AUTHANSWER_RESP_OK message containing the SIGNresult):

communicating a GPRS Attach Complete message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Complete message from the access point to the GPRS authentication element; and followed by the step of (Haverinen column 24, lines 25-38: (Step 453) The MT receives the PAC_MT_AUTHANSWER_RESP_OK message and checks the SIGNresult it contains. If the SIGNresult is correct, the MT can inform the user of the start of billing):

communicating an authentication success message from the GPRS authentication element to the access point, and the step of authorising the access port for GPRS communication in

response to receiving the authentication success message (Haverinen column 24, lines 34-35: If it does not re-authenticate, the connection of the MT to the PAC is released and the MT can authenticate itself again).

As to claim 19, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the local network is a Wireless Local Area Network (WLAN) (Haverinen column 18, lines 40-44: The MT has an equipment part ME and SIM_B provided for use with the second GSM telecommunications network GSM_B. The MT may not be a GSM compliant mobile station. In this case a user of the MT can access the second GSM telecommunications network GSM_B by providing a GSM mobile station with the SIM_B. Indeed, in this example, the MT is a laptop computer equipped with a WLAN adapter card (not shown) and a smart card reader (not shown) that can use the SIM_B. Alternatively, the MT is a device having a GSM mobile station part for communicating with GSM telecommunications networks and a WLAN terminal part for communicating with WLANs).

As to claim 21, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the local network authentication messages are extensible authentication messages (Haverinen Figure 16).

As to claim 22, Haverinen discloses a method of authenticating as claimed in claim 1 wherein the local network authentication messages are Extensible Authentication Protocol messages (Haverinen Figure 16).

As to claim 25, Haverinen discloses a communication system comprising a GPRS communication network and a local network, the communication system comprising: means for a GPRS communication unit to attach to the access point using a local network protocol;

(Haverinen column 9, lines 56-63: The actual type of the telecommunications network is irrelevant. GSM is used as an example, but the network type could as well be Universal Mobile Telecommunications System (UMTS) or GSM with General Packet Radio Service (GPRS). Actually, GPRS can be understood as an extension to GSM rather than an independent network in the sense that GPRS operates using GSM radio access network and GSM authentication methods);

and means for authenticating the GPRS communication unit by communicating GPRS authentication messages between the GPRS communication unit and a GPRS authentication element through the access point by encapsulation of GPRS authentication messages in local network authentication messages (Haverinen column 3, lines 5-41: According to a first aspect of the invention there is provided an authentication method for authenticating a mobile node to a packet data network, comprising the steps of: providing the mobile node with a mobile node identity and a shared secret specific for the mobile node identity and usable by a telecommunications network; providing the mobile node with a protection code; sending the mobile node identity and the protection code from the mobile node to the packet data network; providing the packet data network with authentication information usable by the telecommunications network, the authentication information comprising a challenge and a session secret corresponding to the mobile node identity and derivable using the challenge and the shared secret; forming cryptographic information using at least the protection code and the session secret; sending the challenge and the cryptographic information from the packet data network to the mobile node; checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret; generating at the mobile node the session

secret and a first response corresponding to the challenge, based on the shared secret; sending the first response to the packet data network; and checking the first response for authenticating the mobile node).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 20, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7107620 (Haverinen) as applied to claim 1 above, and further in view of US 20030119481 (Haverinen2).**

As to claim 20, Haverinen discloses a method of authenticating as claimed claim 15. Haverinen fails to teach wherein the Wireless Local Area Network (WLAN) conforms to the Institute of Electrical and Electronic Engineers standard no. 802.1x.

However, Haverinen2 discloses wherein the Wireless Local Area Network (WLAN) conforms to the Institute of Electrical and Electronic Engineers standard no. 802.1x (Haverinen2 page 2, paragraph 0015: According to a preferred embodiment, the local network BAN is a wireless local area network employing user authentication and access control according to IEEE 802.1x standard…).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Haverinen and Haverinen2 because 802.1x is just a standard that can be

applied to a WLAN (Haverinen2 page 2, paragraph 0015: According to a preferred embodiment, the local network BAN is a wireless local area network employing user authentication and access control according to IEEE 802.1x standard…).

As to claim 23, Haverinen discloses a method of authenticating as claimed in claim 1. Haverinen fails to teach wherein the GPRS authentication element is a Serving GPRS Support Node (SGSN).

However, Haverinen2 discloses wherein the GPRS authentication element is a Serving GPRS Support Node (SGSN) (Haverinen2 page 2, paragraph 0021: Even though the authentication server is shown as a separate element in FIG. 1a, it can be implemented for example as a part of a service node BSN, the SGSN or the GGSN.

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention an authentication element/server could be a SGSN (Haverinen2 page 2, paragraph 0021: Even though the authentication server is shown as a separate element in FIG. 1a, it can be implemented for example as a part of a service node BSN, the SGSN or the GGSN.

As to claim 24, Haverinen discloses a method of authenticating as claimed in claim 1. Haverinen fails to teach wherein the GPRS communication unit is a dual-mode communication unit operable to communicate in accordance with a GPRS protocol and a local network protocol.

However, Haverinen2 discloses wherein the GPRS communication unit is a dual-mode communication unit operable to communicate in accordance with a GPRS protocol and a local network protocol (Haverinen2 page 3, paragraph 0037: According to a preferred embodiment, the MS is a dual-mode terminal, which is also able to connect not only to the local network BAN but also to a UMTS network via UTRAN base stations (node B)).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that if the terminal/GPRS communication unit could operate in dual-mode then it would not matter what the protocol was (Haverinen2 page 3, paragraph 0037: According to a preferred embodiment, the MS is a dual-mode terminal, which is also able to connect not only to the local network BAN but also to a UMTS network via UTRAN base stations (node B)).

Prior Art

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 6512756 is pertinent because it teaches the invention relates to a cellular packet radio network and to a method for updating a routing area in a packet radio network...There is a logical link between a mobile station (MS) and a serving packet radio support node (SGSN)...The update request includes the identifiers of the old and new routing area. When the packet radio node detects a routing area update carried out by an unknown mobile station, it initiates the establishment of a logical link by sending a link establishment message (LLC Subm, 21, 21') to the mobile station, the message including the same identifier the mobile used for itself in the routing area update request. The mobile station initializes the logical link at its own end and sends and acknowledgement to the serving packet radio support node. US 6940869 is pertinent because it teaches… an integrated system is formed of portions of a GPRS system as well as portions of a WLAN system, such as that defined in the IEEE 802.11 standard. A WIP (WLAN Integrated Protocol) layer is defined, functionally positioned between upper-level, GPRS layers and lower-level, WLAN layers. Advantages of a GPRS system as well as advantages of the WLAN system are maintained in the integrated system. US 7050416 is

pertinent because it teaches… Associated with one or more of the access networks is a corresponding one of a plurality of Serving GPRS Service Nodes (SGSNs) (24.sub.1 24.sub.m), each node serving to identify and authenticate a mobile terminal user. Advantageously, each SBSN also serves to cache IP packets from a sending mobile terminal user and to examine each packet to determine if the destination IP address corresponds to another mobile terminal user in the network. If so, then that SGSN routes the packet to the destination mobile terminal user. Otherwise, if the packet destination lies outside the network, the SGSN routes the packet to a gateway (32) for routing beyond the network.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/

/R. L. P./

Examiner, Art Unit 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136